NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Scouring endangers U.S. river pipelines. Soil on the bed of the Missouri River was washed away by floodwaters, exposing and rupturing a natural gas pipeline, an energy company said. A pipeline owned by Enterprise Products Partners spilled about 3,300 barrels of natural gas liquids into a flooded area of the Missouri River the weekend of August 13 and 14 in Iowa. Flooding along the river exposed several pipelines to danger after rushing waters swept away several feet of the river bed. State officials in North Dakota last month found evidence of scouring 30 feet deep. Federal law requires pipelines be buried 4 feet below the riverbed. An Enterprise spokesman was quoted by The Wall Street Journal as saying scouring exposed most of the pipeline near Onawa, Iowa. Magellan Midstream Partners, another pipeline company, announced it suspended operations at one of its pipelines crossing the Missouri River because of scouring fears. The U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration in July called on pipeline operators to look into the potential effects of scouring. Source: http://www.upi.com/Business_News/Energy-Resources/2011/08/19/Scouring-endangers-US-river-pipelines/UPI-14141313754900/

Jamestown officials to begin diking in response to increased reservoir releases due to rain. Officials in Jamestown, North Dakota, said diking will be necessary in parts of the city due to increased water releases from the Jamestown and Pipestem reservoirs located north of the city. Heavy rains forced the U.S. Army Corps of Engineers to up the increases, the largest releases in 2 years, according to the Jamestown Sun. A city engineer said he anticipates 2,700 feet of dikes will be up by the end of the week of August 22. He said about a third of it will be what he considers major diking. Source: http://www.therepublic.com/view/story/dbfac7e08625466aabdbcb12a1c6fd9b/ND--ND-Flooding-Jamestown/

Garrison Dam releases fall. Missouri River water releases at Garrison Dam in North Dakota dropped below 100,000 cubic feet per second (cfs) for the first time since May 31. The Bismarck Tribune reported the U.S. Army Corps of Engineers lowered dam releases to 95,000 cfs August 12, and planned to close the dam's spillway gates August 17 after it stepping down releases to 85,000 cfs. The Corps opened the spillway gates for the first time in the dam's half-century history June 1 due to swollen Missouri River levels. The Bismarck Tribune reported that the river's height was 17.06 feet at 9 p.m. August 12. Flood stage is 16 feet. Source: http://www.jamestownsun.com/event/article/id/142095/group/News/

Regional

(Minnesota) **Suspicious package evacuates building at Inver Hills Community College.** The science building at Inver Hills Community College in Inner Grove Heights, Minnesota remained closed late in the afternoon August 16 after a suspicious package was found inside the building earlier in the day. The college's director of marketing said the package was discovered around 10 a.m., and security was notified immediately. The building was evacuated as officials investigated. The director said college was not in session yet, and that only a few staff members

were in the building at the time. The package was taken off site for further examination. Officials said the building would reopen once that evaluation was complete. Source: http://ksax.com/article/stories/S2243351.shtml?cat=10230

(Montana) **Yellowstone oil spill cleanup will last into fall.** The cleanup of a major oil spill in the Yellowstone River has proven more difficult than expected and could go on for several more months, an Exxon Mobil Pipeline Co. executive said August 18. Areas hit hardest by the July spill should be cleaned up by the first half of October, said the company vice president. That includes a 20-mile stretch of the Yellowstone stretching from the spill site near Laurel downstream to Billings, Montana. But scattered sites still would need to be dealt with, including contaminated river sections downstream of Billings, and two large islands in the heavily impacted area. Slowing the cleanup effort has been the painstaking task of removing crude from hundreds of debris piles deposited by the same spring floodwaters widely believed to have triggered the 12-inch pipeline's failure. Also, the energy company did not want to bring in more workers than necessary to avoid trampling the riverbank, he said. The U.S. Environmental Protection Agency on-scene coordinator said the cleanup "is much more dictated by progress in the field instead of a date on the calendar." He added that final approval of the work done by Exxon Mobil would have to come from Montana officials. About 1,000 people are involved in the effort to mop up the spill, including roughly 850 Exxon Mobil employees and contractors working along dozens of miles of riverbank. Source: http://news.yahoo.com/yellowstone-oil-spill-cleanup-last-fall-192356928.html

(South Dakota; Nebraska) **Reservoirs fall below flood levels.** The Missouri River flood fight reached a milestone when the last of the six big upstream reservoirs, Fort Randall in South Dakota, fell to its normal full level August 17. "Our goal has always been to evacuate all the flood-control storage before the 2012 runoff season begins, and we are on our way to achieving that," said an official from the U.S. Army Corps of Engineers. All of the reservoirs on the upper Missouri are now out of what the Corps calls the "exclusive flood control zone." The six reservoirs held 66.3 million acre-feet of water August 17. The Corps plans to bring the storage down to 56.8 million acre-feet before March 1 to provide enough room for next year's runoff. "There is still high water on the levees and in the flood plain, and while this is the first step toward decreasing the water level, we need to stay vigilant until the water recedes," said the Omaha District commander. Releases from Gavins Point Dam on the Nebraska-South Dakota border are at 150,000 cubic feet per second (cfs). Releases are expected to be 40,000 cfs by the end of September. Source: http://www.omaha.com/article/20110818/NEWS01/708189906

National

President Obama signs new Executive Order isolating the government of Syria from the U.S. financial system, imposes sanctions against Syria's energy sector. The U.S. President signed an Executive Order (EO) imposing additional sanctions against the Government of Syria August 18, freezing any assets of the Government of Syria in the United States and banning the importation into the United States of petroleum or petroleum products of Syrian origin. Responding to the continuing escalation of violence against the people of Syria, the EO reflects

the ongoing commitment of the United States to ensure any assets of the Syrian government subject to U.S. jurisdiction cannot be used to further the Syrian regime's campaign of violence and repression against Syrian citizens. The EO significantly escalates financial pressure on the Government of Syria, which includes its agencies, instrumentalities, and controlled entities, by denying it access to the U.S. financial system, and prohibiting U.S. persons from engaging in transactions or dealings with it. Source: http://www.treasury.gov/press-center/press-releases/Pages/tg1280.aspx

INTERNATIONAL

Somali pirates hijack chemical tanker anchored in Omani waters. Somali pirates hijacked a chemical tanker within 3 nautical miles of the Omani port of Salaleh, the first seizure within territorial waters and while a vessel was at anchor, the International Maritime Bureau said. Armed pirates boarded the Fairchem Bogey August 20, taking 21 crew hostage and putting the vessel on course for Somalia, according to the bureau's Piracy Reporting Center. Attacks on vessels by Somali pirates operating in the Gulf of Aden and the Indian Ocean, an area as large as Europe, rose to a record in 2011's first half, according to the International Maritime Organization, the United Nations' shipping agency. Piracy costs the global economy an estimated $7 billion to $12 billion a year, the IMO says. The president of Fairfield Japan Ltd., the Japanese subsidiary of Roseland, New Jersey-based vessel owner Fairfield- Maxwell Services Ltd., confirmed the hijack. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2011/08/22/bloomberg1376-LQBKYK07SXKX01-2H5E93K60QQAFGB0VH17KS7EKE.DTL

U.N. atom body wants wider nuclear safety checks. The United Nations (U.N.) atomic agency would carry out international safety checks of 10 percent of the world's reactor units over a 3-year period, under a draft action plan to prevent any repeat of Japan's nuclear crisis. The document from the International Atomic Energy Agency (IAEA), obtained by Reuters August 15, outlined a series of measures in 10 areas to help improve global nuclear safety after the Fukushima accident more than 5 months ago. While stressing atomic energy safety was primarily a national responsibility, it signaled a strengthened role for the IAEA to review compliance with international reactor and regulatory standards. Among the proposed steps in the Nuclear Safety Action Plan, the IAEA would "organize operational safety reviews ... of one nuclear power unit in ten over a period of three years". It did not give details, but the IAEA has previously suggested plants could be randomly selected for such checks. There are some 440 operating nuclear reactors in the world. The agency would also conduct regular assessments of national regulatory bodies, the draft said, in an apparent attempt to make sure they were sufficiently independent and resourced to be able to work effectively. The proposals, aimed at ensuring nuclear plants can withstand extreme events such as the earthquake and tsunami that crippled Fukushima, may prove controversial for countries that want to keep safety an issue strictly for national authorities. The draft builds on the outcome of an IAEA-hosted nuclear safety conference in June. It will be discussed by diplomats of the agency's member states ahead of the U.N. body's decision-making General Conference next month. Source: http://www.reuters.com/article/2011/08/15/nuclear-iaea-safety-idUSLDE77E0F720110815

Criticism grows over Shell's handling of oil leak. Pressure mounted August 16 on Royal Dutch Shell to explain how 1,300 barrels of oil could have leaked from a pipeline into the North Sea, after the spill, which was discovered last week, tarnished a widely praised record for avoiding such incidents in England. Shell said it was still working on finding the source of a smaller leak from the same part of the pipeline that connects a well with the Gannet Alpha platform about 122 miles east of the Scottish city of Aberdeen. About one barrel a day was still leaking into the sea, Shell said. The British Department of Energy and Climate Change said the spill was "substantial" in the context of the U.K. Continental shelf. Shell's technical director in Britain, also said it was a "significant spill in the context of annual amounts of oil spilled in the North Sea." The broken pipeline allowed about 218 tons of oil to flow out, making it the biggest leak in British waters for a decade. An oil sheen now covers about 10 square miles of water, the company said. Shell said August 16 it had shut the well and depressurized the pipeline, reducing the amount of oil that could still leak into the water to a finite amount, the company said. The leak was "under control," Shell said. On August 16, Shell was under pressure to disclose the reason for the spill and to stop any oil flowing into the sea after it emerged that the company had waited 3 days to issue a public statement about the leak even though it had informed the authorities. Shell said it had started an investigation into the spill and was still working to establish its cause. The amount of oil spilled through Gannet Alpha is more than four times the total amount of oil spilled into British waters last year. The rig is operated by Shell on behalf of itself and Esso Exploration and Production, a unit of Exxon Mobil. Source: http://www.nytimes.com/2011/08/17/business/global/criticism-grows-over-shells-handling-of-oil-leak.html

Banking and Finance Industry

Auditors: IRS plan compromises security for e-payment users. The Internal Revenue Service (IRS) glossed over computer security in planning for a new tax return law that applies to e-payment processors, government investigators said in a report released August 18. The agency's strategy for applying the law "does not consider the security of the computer systems being planned and changed or the new data being received," the Treasury Inspector General for Tax Administration's (TIGTA) deputy inspector general for audit wrote in a July 26 report released August 18. The new provision will require the IRS to store the names, addresses, and taxpayer identification numbers, or TINs, of the sellers that each third-party processor submits. Small vendors often use their Social Security numbers as their TINs, so the reporting could put them at greater risk of identity theft, say some privacy groups, such as the Center for Democracy and Technology. On August 19, a TIGTA spokesman said the IRS has since informed auditors that, after the review, the agency added particulars on computer security to its roll-out plan. Source: http://www.nextgov.com/nextgov/ng_20110819_2747.php

Better ATM skimming through thermal imaging. Security researchers found thermal cameras can be combined with computer algorithms to automate the process of stealing payment card data processed by automatic teller machines. At the Usenix Security Symposium the week of August 8, the researchers said the technique has advantages over more common ATM

skimming methods that use traditional cameras to capture PINs people enter during transactions. The reason is customers often obscure a traditional camera's view with their bodies, inadvertently or on purpose. Also, it can take a long time for crooks to view captured footage and log the code entered during each session. Thermal imaging can vastly improve the process by recovering the code for some time after each PIN is entered. The output can also be processed by an algorithm that automates the process of translating it into the secret code. The findings expand on 2005 research from a member of Google's security team. The Usenix presenters tested the technique laid out by the researcher on 21 subjects who used 27 randomly selected PINs, and found the rate of success varied depending on variables such as the types of keypads and a person's body temperature. Source: http://www.theregister.co.uk/2011/08/18/thermal_imaging_atm_fraud/

New FDIC phishing attack. The Federal Deposit Insurance Corporation has fallen victim to a phishing attack through fake e-mails that urge business owners to click links purporting to provide FDIC data about their financial institutions. Fraudulent e-mails are being sent from alert@fdic(dot)gov with the subject line: "FDIC: Your business account." In a consumer alert, the FDIC said the scheme's wording varies slightly from other scams. Some e-mails begin with "Dear Business Owner," instead of "Dear Business Customer." The e-mails also say, "We have important news regarding your bank," instead of, "We have important news regarding your financial institution." Fake e-mails are also coming from subscriptions@fdic(dot)gov. The fraudulent e-mails say business accounts and loans might be affected by acquiring-bank relationships, offering vendors information about how they can file claims against the receivership. "The FDIC does not issue unsolicited e-mails to consumers or business account holders," the FDIC alert states. Source: http://www.bankinfosecurity.com/articles.php?art_id=3972

Fake blocked credit card e-mails carry malware. Security researchers from Sophos have intercepted a new malware distribution campaign that generates e-mails posing as blocked credit card notifications from MasterCard. The rogue e-mails bear titles like "Your credit card is blocked" or "Your credit card has been blocked", and have spoofed headers to appear as originating from a @mastercard(dot)com address. Their content claims the recipient's credit card was charged in a fraudulent manner which led to it being blocked. The messages signed by MASTERCARD(dot)com Customer Services read: "Dear Customer, Your credit card is blocked! Your credit card was withdrawn $#### Possibly illegal operation!" The e-mails instruct users to open the attached document to learn more information and contact their respective banks as soon as possible. The attachments, ZIP archives with random numerical names, contain installers for Bredolab variants. Trojans from the Bredolab family act as malware distribution platforms so victims may get multiple infections. Security researchers note similar e-mails purporting to come from VISA or other credit card companies have also been spotted. Source: http://news.softpedia.com/news/Fake-Blocked-Credit-Card-Emails-Carry-Malware-217142.shtml

Phishing scam targets IRS. Phishing e-mails, feigning to be from the Internal Revenue Service, are reportedly targeting consumers with claims tax accounts have been locked and require

immediate action to reopen. The e-mails, which appear to come from info manager@irs(dot)gov and support manager@irs(dot)gov, according to other news accounts, are the latest in a round of phishing attacks aimed at the IRS. The e-mails reportedly are not so sophisticated, often containing numerous typos. When reached for comment, the IRS would not discuss this specific attack, but did provide a link to a list of known e-mail scams targeting consumers under the guise of the IRS. The IRS is a relatively easy target because of its name recognition among consumers, many of whom might not readily recognize a phishing scam. In this most recent case, the phishy e-mails ask recipients to fill out and mail an attached notification back to the IRS, along with accompanying documents, such as copies of U.S.- or state-issued photo I.D.s. Similar phishing attacks reported to the IRS have been more traditional, including malicious links and/or attachments rather than also asking consumers to mail personally identifiable information to a physical address. Source: http://www.bankinfosecurity.com/articles.php?art_id=3965

GAO: FDIC cybersecurity lacking. The confidentiality and integrity of the Federal Deposit Insurance Corporation's (FDIC) information systems are vulnerable, said a Government Accountability Office (GAO) report published August 12. Weak passwords, poor user-access policies, inconsistent encryption and unsatisfactory patch implementation threaten the FDIC's financial systems and databases, the GAO found. While security risks persist at the FDIC, the situation is an improvement when compared to past cybersecurity problems at the agency. FDIC remediated 26 of the 33 control weaknesses the GAO identified in a similar 2009 audit, the government watchdog found. However, the report authors noted, "the corporation did not always fully implement key information security program activities, such as effectively developing and implementing security policies." The GAO suggested the FDIC develop, document, and implement information security fixes for its loss-share loss estimation process. The GAO also made 38 new cybersecurity recommendations to address 37 findings from the audit, which were outlined "in a separate report with limited distribution," report authors wrote. Source: http://www.fiercegovernmentit.com/story/gao-fdic-cybersecurity-lacking/2011-08-15

Global card fraud ring busted. New South Wales (NSW) Police in Australia said the department's fraud squad has arrested and charged five Malaysian and Sri Lankan nationals suspected of being behind an elaborate international card-skimming scheme that spanned the United Kingdom, mainland Europe, and North America. The alleged scheme, which authorities have been investigating for several months, involved skimming at point-of-sale terminals in numerous merchant locations. Police did not say how the accused are suspected of pulling off the scam, but did say authorities seized numerous point-of-sale (POS) terminals, PIN overlays, and other electronics, such as laptops and mobile phones. Authorities also discovered $10,000 in Canadian dollars, falsified identification and travel documents, and a number of Canadian credit cards. Over the last several months, investigators in connection with the case have seized more than 50 stolen POS terminals, dozens of skimmers, and more than 18,000 blank and counterfeit cards. So far, 25 people have been arrested and charged. Source: http://www.bankinfosecurity.com/articles.php?art_id=3963

Chemical and Hazardous Materials Sector

IAEA describes atomic security steps in 2010. The International Atomic Energy Agency (IAEA) in a newly issued report said it took continued steps to advance the protection of nuclear materials in 2010. The U.N. nuclear watchdog reported carrying out 17 "nuclear security advisory missions" last year. "More than half dealt with physical protection and with legal, regulatory and practical measures for controlling nuclear and other radioactive material," according to the document. "Several additional missions reviewed the arrangements by states for detecting illicit nuclear trafficking and for responding to nuclear security emergencies and incidents," it added. To assist states in developing human resource capabilities in the area of nuclear security, the agency conducted 172 training events involving the participation of more people from 120 countries, the report added. The assessment is one of many documents furnished to the IAEA General Conference, a body comprised of all of the U.N. agency's member states, according to an August 12 news release. Source: http://www.globalsecuritynewswire.org/gsn/nw_20110815_2717.php

Russia builds Iran's first nuclear power plant. Iran's first nuclear power plant, built by Russia, will be connected to the national grid in late August, the atomic chief told the Arabic-language network Al-Alam August 14. "The test to reach 40 percent of the plant's power capacity has been done successfully ... God willing, we will be able to commission the plant by the end of Ramadan with an initial production" of the same amount, he said. He estimated that the plant would reach its "full capacity of 1,000 megawatts" in late November or early December. Source: http://nation.foxnews.com/iran/2011/08/15/reset-russia-builds-irans-first-nuclear-power-plant

Commercial Facilities

(New York) **Guilty plea in Times Square bomb case.** A New York man pleaded guilty in federal court August 18 to running an unlicensed money transfer business between the United States and Pakistan. One of the money transfers facilitated by the suspect was used to fund the May 1, 2010, attempt by a man to set off a car bomb in Times Square, the U.S. Department of Justice (DOJ) said. That man is serving a life sentence in federal prison for the attempted bombing. The suspect who pleaded guilty operated a “hawala,” a sort of informal system of transferring monetary value without physically transferring money across international borders. He conducted two transactions April 10, 2010 that provided thousands of dollars to two customers “at the direction of a co-conspirator in Pakistan, but without knowledge of how the customers were planning to use the funds,” the DOJ said in a news release. The suspect faces a maximum prison sentence of 5 years and a maximum fine of $250,000, or double the gain or loss arising from his conduct, the release said. He is scheduled to be sentenced November 30. Source: http://www.upi.com/Top_News/US/2011/08/18/Guilty-plea-in-Times-Square-bomb-case/UPI-33641313725788/

(Arizona) **Pipe bomb explodes near Tucson facility.** Police were investigating a pipe bomb explosion that sent a piece of shrapnel through the bedroom window of a Tucson, Arizona, assisted living facility August 16. Officers responded to the scene and found pieces of debris and shrapnel near the assisted living facility and in the roadway. The Arizona Daily Star said

police eventually found the location of the blast near the doorway of a business. Police have submitted the evidence to have it forensically analyzed and determine the composition of the explosive material. A motive has not been determined, and police do not have any suspects. Source: http://ktar.com/category/local-news-articles/20110818/Pipe-bomb-explodes-near-Tucson-facility/

Communications Sector

Nothing Significant to Report

Critical Manufacturing

NHTSA recall notice - Chevrolet Impala. General Motors (GM) is recalling 10,344 model year 2012 Chevrolet Impala vehicles manufactured from April 19, 2011, through July 29, 2011. The upper power steering hose may have been misrouted so that it can come in close proximity to and/or contact the catalytic converter. With the engine on, heat from the catalytic converter may melt the power steering hose. Power steering fluid could flow onto the catalytic converter, and an engine compartment fire could occur. GM dealers will inspect to ensure that the upper power steering hose is routed correctly and make the necessary repairs free of charge. The safety recall is expected to begin on or before August 12, 2011. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=11V398000&summary=true&prod_id=1249768&PrintVersion=YES

Defense/ Industry Base Sector

Air Force struggles to keep Pave Hawks in air. It is more difficult than ever to keep the 30-year-old Pave Hawk helicopter flying, and U.S. Air Force officials estimate only 57 percent of the combat search-and-rescue fleet will be available for missions at any given time in 2011, Air Force Times reported August 20. The HH-60 is being flown twice as often as it was designed to fly, and it is taking a toll on the aircraft. The commander of Air Combatant Command (ACC) said the service was looking for budget solutions to replace the entire fleet of 99 remaining Pave Hawks, but as a stop-gap, the Air Force was using appropriated funds to replace 13 aircraft lost in combat or retired. He said the HH-60s, which cost $26 million apiece, are often called upon because of their versatility and because they do not require special clearances needed by other aircraft to fly downrange. The Air Force announced in April that half the fleet was undergoing repairs to major structural cracks that made the HH-60s unsafe to fly. The cracks were primarily in the "308 beam," which stretches over the roof of the helicopter and bears as much as 20,000 pounds when the chopper is fully loaded. "The HH-60G Pave Hawk is a severely stressed aircraft showing the impacts of its demanding mission," an ACC spokeswoman said. The mission-capable rate for fiscal 2010 was 59 percent and availability for fiscal 2011 is trending toward 57 percent, she said. Air Force officials said in April that by 2015, the mission-capable rate would dip below 50 percent. Source: http://www.airforcetimes.com/news/2011/08/air-force-pave-hawks-keep-in-air-082011w/

DoD to expand cyber program with industry. The U.S. Defense Department (DOD) is moving forward with a program designed to increase sharing with industry of classified and sensitive data about cyberattacks, the Deputy Secretary of Defense announced August 16. A 3-month pilot program — the Defense Industrial Base Cyber Pilot — has "stopped hundreds of attempted intrusions," he said at a Defense Information Systems Agency conference. It also appears to be cost effective, he added. The program will be extended beyond its original end date of September 30. About 20 companies initially volunteered to participate in the pilot. "In the coming months, we will expand the pilot to the rest of the industrial base, as well as other key areas of critical infrastructure," the deputy said. In addition to thwarting attacks against contractors, DOD said it identified strings of malware used by hackers. That information was incorporated into DOD network defenses and shared with companies participating in the pilot. Knowledge of these malware signatures "dramatically increases the effectiveness of cybersecurity," the deputy said. DOD and its contractors must seize the current "window of opportunity" to strengthen their networks against destructive cyber threats, that if launched, would cause great physical damage and even loss of life, he said. Source: http://www.defensenews.com/story.php?i=7416591&c=AME&s=TOP

Emergency Services

(California) **Hacker group threatens Fullerton PD, compromises BART website.** A group of hackers calling itself "Anonymous" responsible for threats against the Fullerton, California Police Department, has also claimed to be behind a security breach of user information on a Web site for the San Francisco Bay Area Rapid Transit. The group sent a letter to the Fullerton Police Department announcing it would avenge a recent death by treating the police Web site "with as much mercy as was shown Kelly Thomas." They also threatened to disable the agency's Web site if the officers involved in the alleged beating were not prosecuted. Anonymous was demanding the immediate resignation of the police chief, prosecution of the officers involved, and for the city of Fullerton to pay the family of the person beat to death at least $5 million. If the demands were not met by noon August 14, the group said it would shut down the city's police Web site. As of August 14, Fullerton police officials said they had not detected any problems. Police officials said the department wastaking the threat seriously. The city's information technology staff were ordered to secure the department's computers, and to monitor its system for any trouble, a police sergeant told the Los Angeles Times. The same group of hackers was also responsible for hacking into a marketing Web site for the San Francisco Bay Area Rapid Transit August 14, compromising data for hundreds of users. Source: http://www.fox40.com/news/headlines/ktla-hackers-threaten-fullerton-pd,0,6021788.story?track=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Ktxl-Fox40NewsAtTen+(KTXL+-+FOX40+News+at+Ten)

(Pennsylvania) **Verizon strikers allegedly sabotage police station landlines.** State police in Uniontown, Pennsylvania experienced a 29-hour loss of landline phone service when someone shut off the power in underground Verizon vaults around 9:30 p.m. August 9. Police were trying to determine whether or not the act of criminal mischief was related to the ongoing strike by

Verizon landline workers. A police trooper said that there was no forced entry at the sites on Main Street and on Route 119 in Lemont Furnace, near the Penn State Fayette campus. The lack of forced entry has led police to believe that the person responsible for shutting down the power had a set of keys. The local state police were without phone and computer service for 21 hours. Calls had to therefore be forwarded to dispatchers who worked out of another barracks several miles away. Source: http://thejobmouse.com/2011/08/13/verizon-strikers-allegedly-sabotage-landlines-to-police-station/

ENERGY

Energy Dept. says copper thefts on rise. With copper prices at a near record, thieves across the country have been stealing copper wiring from power lines, construction sites, and warehouses. Now federal officials said thieves are targeting power substations and even a locked recycling yard at a nuclear lab. The Energy Department's (DOE) inspector general (IG) reports a "troubling increase" in copper thefts from federal sites, including national research labs, generating stations, and a plant where nuclear weapons are dismantled and stored. An estimated total of $500,000 to $750,000 worth of copper has been stolen from DOE sites in the past 3 years, the IG said. Thefts have ranged from small amounts to about 30,000 pounds of copper stolen from the Los Alamos National Laboratory in New Mexico. In Texas, hundreds of pounds of copper were stolen from the Pantex plant near Amarillo, where nuclear weapons are stored and dismantled. The IG said DOE officials must improve security, especially at recycling facilities and remote substations. In many cases, stolen copper "had not been secured in any way," the IG wrote in a 3-page letter August 18. Some DOE sites had only minimal access controls to areas where copper is stored, he said. In the Los Alamos case, about 30,000 pounds of copper — worth an estimated $120,000 — was stolen from a fenced facility that is locked after hours. Four contractor employees were convicted in the case. Copper was selling for nearly $4 a pound August 17, more than double the price in early 2009. Source: http://moneywatch.bnet.com/economic-news/news/energy-dept-says-copper-thefts-on-rise/6281516/

(Oklahoma) **Okla man arrested for trying to blow up pipeline.** A 40-year-old man has been arrested on accusations he attached an improvised explosive device (IED) to a natural gas pipeline in eastern Oklahoma. The FBI identified the suspect August 12, and said the man acknowledged making and placing the device August 7 on the pipeline, and putting a timer on it set for 2 a.m. The device did not go off and there was no damage. An FBI spokesman said the agency has no motive yet. A federal complaint said the IED was discovered August 10 on a pipeline at the Enerfin Resources substation. Company workers discovered the device. The suspect was arrested on charges of attempting to destroy property used in interstate or foreign commerce. Source: http://news.yahoo.com/okla-man-arrested-trying-blow-pipeline-235750492.html

Bill aims to upgrade security at power plants. A loophole in law does not require workers hired at most power plants to undergo FBI background checks even though a federal report warns the plants are a likely route for terrorists, a U.S. Senator said August 14 in unveiling legislation

that would change that. The New York Senator cited a recent DHS report that found disgruntled former employees have sensitive inside information that would be sought by terrorists. The report also said current employees have been solicited by unidentified outsiders. In the fall of 2010, al-Qa'ida urged recruits to take jobs in potential terrorist targets such as power plants where they could inflict significant damage and chaos quickly and easily, the report noted. The Senator's bill would require FBI background checks on all employees of major power plants. The Senator said the report shows that al-Qa'ida is recruiting terrorists to work in sensitive locations such as electric, gas, and water utilities. Source: http://www.thetimesherald.com/article/20110814/NEWS05/110814008

Food and Agriculture

(North Carolina; South Carolina; Virginia) **Blue plastic chips found in ground beef.** Vantage Foods of Lenoir, North Carolina, recalled 1,642 pounds of ground beef after a consumer found blue plastic chips in the product. The U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service announced the recall August 19. Products included in this Class III recall — the type issued when consumption of the product will not cause adverse health consequences — were sold in 2-pound trays of fresh ground beef 93/7 under the brand "Lowe's Foods." The packaging is labeled with Establishment number "EST. 34176" inside the USDA mark of inspection, and a sell-by date of 8/29/11. The products subject to recall were produced August 15, and distributed to retail stores in North Carolina, South Carolina, and Virginia. The problem was discovered when a consumer returned meat to a retail establishment, reporting the presence of blue plastic chips in the product. The store then notified Vantage Foods. Source: http://www.foodsafetynews.com/2011/08/blue-plastic-chips-found-in-ground-beef/

Japan finds first case of radioactive contamination in rice. Japanese inspectors found the first case of radioactive contamination in rice August 19, adding the national grain to the list of foods harmed by the accident at the stricken Fukushima Daiichi nuclear plant. Inspectors in Ibaraki Prefecture, just north of Tokyo, found radioactive cesium in a sample of rice from the city of Hokota, about 90 miles south of the radiation-spewing nuclear plant. The prefecture said the radiation was well within safe levels: It measured 52 becquerels per kilogram, about one-tenth of the government-set limit for grains. The prefecture said two other samples tested at the same time showed no contamination. The Agriculture Ministry said this was the first time that more than trace levels of cesium had been found in rice, though it said there was no health risk. Source: http://www.nytimes.com/2011/08/20/world/asia/20rice.html

USDA inspectors to enforce humane treatment of animals. Meat inspectors at federally regulated plants that slaughter animals received new instructions for humane treatment of animals. Announced by the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS), the rules will go into effect September 15. The directive on enforcement of humane handling codifies changes made in the last few years to ensure animals going to slaughter are treated properly. The new version, which FSIS says will require additional training for meat inspectors, includes a definition for "egregious inhumane handling" of animals — "any act or condition that results in severe harm to animals, which includes the excessive beating or

prodding of disabled livestock, stunning animals and allowing them to regain consciousness, or any treatment causing unnecessary pain and suffering." The directive provides inspectors with "verification instructions" to ensure treatment of livestock during handling and slaughter "minimizes the animals' amount of excitement, pain, injury, or discomfort." Source: http://journalstar.com/news/state-and-regional/article_6b303c9e-2b34-5ee9-8b1c-d84e4211f45b.html

(Texas) **Texas ag losses forecast at record $5.2 billion.** Texas cattle producers could take several years to fully recover from the drought blistering the state, which agriculture officials estimated August 17 has caused a record $5.2 billion in livestock and crop losses since the fall of 2010. Officials said producers in the nation's leading cattle state have sent more animals than usual to auction because there is nothing for them to graze on. That means fewer animals available to buy down the road, and they will cost more because there will be fewer around. It will also take time before ranchers will have new animals to sell, a Texas AgriLife Extension Service drought specialist said. Drought has spread over much of the South this year, setting records from Louisiana to New Mexico. But the situation is especially severe in Texas, the nation's second-largest agriculture state behind California. Field surveys from November 2010 to August 1, 2011, indicate livestock losses of $2.1 billion and crop losses of $3.1 billion in the state, an extension service economist said. By the time crops are fully harvested, the losses might be higher. Source: http://news.yahoo.com/texas-ag-losses-forecast-record-5-2-billion-162704078.html

(Alaska) **Moth infestation casts pall on Alaska berry crop.** The year's blueberry season in Alaska's most populous region is a bust because of a plethora of leaf-eating caterpillars, Alaska pest management officials said. A multi-year infestation of geometrid moths appears to be peaking in the south-central region, which includes Anchorage, according to a mid-summer advisory by the University of Alaska Fairbanks Cooperative Extension Service. The moths, in caterpillar form, have munched blueberry bushes to the point where they cannot bear fruit, the service said. The moth infestation, and resulting poor berry growth, has occurred in the state's southeast panhandle too. Caterpillars have also defoliated bushes that would normally bear ripe salmonberries, a raspberry-type fruit, and denuded willows, alders, and birch trees, the extension service said. Even though the plants munched by the caterpillars lack many of their leaves and berries, they are most likely not dead and are expected to recover once the infestation is over, the extension service added. Bears also depend on berries, so Alaskans might expect additional raids this fall by bears on trash cans and fish scraps, one state biologist said. Source: http://news.yahoo.com/moth-infestation-casts-pall-alaska-berry-crop-230949117.html

Listeria prevalence in meat, poultry declines. Listeria prevalence in all ready-to-eat meat and poultry products was 0.28 in 2010, according to data released by the Food Safety and Inspection Service (FSIS). This is down from 0.37 in 2009 and represents an 81 percent decline since 2000. This data includes information from all three FSIS sampling projects. FSIS analyzed 3,153 and 8,704 samples for L. monocytogenes in its ALLRTE and RTE001 sampling

projects, respectively. Ten positive samples were observed in ALLRTE (0.32 percent positive), and 24 positive samples were observed in the in RTE001 samples (0.28 percent positive). FSIS analyzed 1,854 products for L. monocytogenes in the RLm sampling program in CY 2010. The sampling results produced four positives samples, resulting in a 0.22 percent positive rate. Source: http://www.wisconsinagconnection.com/story-national.php?Id=1724&yr=2011

(Virginia) **Virginia company recalls cheese spread due to possible salmonella contamination.** The Food and Drug Administration (FDA) announced August 12 that Miss Bonnie's Gourmet, LLC, a Winchester, Virginia company, recalled its Miss Bonnie's Gourmet Classic Cheddar Cheese Spread because it has the potential to be contaminated with Salmonella. The product was distributed between August 1 and August 10, 2011, with a "Best By Date" of December 23, 2011. The Virginia Department of Agriculture and Consumer Services discovered the Salmonella contamination through a routine sampling of the company's products. The recalled product is packaged in 8 ounce glass jars and was distributed to Kroger Stores in Roanoke, Virginia; Cincinnati, Ohio; Louisville, Kentucky; and Memphis, Tennessee. No illnesses associated with this recall have been reported to date. Source: http://www.foodpoisonjournal.com/food-recall/virginia-company-recalls-cheese-spread-due-to-possible-salmonella-contamination/

(Oregon) **More evidence seen that deer spread Oregon e. coli.** Health officials said they think they will be able to prove deer droppings in a strawberry field in Oregon caused an E. coli outbreak that killed one person and sickened 14 others. Ten percent of the samples taken from the Jaquith Strawberry Farm in Newberg tested positive for the bacteria, an epidemiologist said August 11. Scientists tested more than 100 samples of soil, strawberries, and deer droppings found in the field in Washington County. The Oregonian reported the lab has yet to confirm a match in the specific strain of E. coli bacteria. "We're increasingly confident that we will be able to prove beyond any reasonable doubt that deer were the source of contamination of the strawberries," the epidemiologist said. Scientists were surprised such a high percentage of the samples tested positive. Bacteria is never uniformly spread throughout the environment or on contaminated food. Sometimes epidemiologists know it is there but can not prove it in the laboratory. Of the 15 people involved, two suffered kidney failure, including an elderly woman in Washington County who died. Two patients remained in the hospital, the newspaper reported. Source: http://abcnews.go.com/Business/wireStory?id=14291764

Two recalls announced due to Listeria contamination. On August 12, the Food and Drug Administration (FDA) and the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced the recall of products possibly contaminated with Listeria monocytogenes. After a routine sampling by the FDA, Listeria monocytogenes were found in the imported avocado pulp used in various Layer Dip products made by Fresh Food Concepts, Inc. of Buena Park, California. The products affected were distributed to supermarkets and club stores throughout the United States and Canada. The company noted that their products with use by dates of September 24, 2011 and after are made with avocado from a different source and are not involved in the recall. Fresh Food Concepts, Inc. ceased the use of avocado from the supplier. In addition, the FSIS announced August 12, that the Canadian company, Ailments

Prince, S.E.C., recalled about 380,000 pounds of diced bacon products that may be contaminated with Listeria monocytogenes. Routine testing July 19 found a sample of cooked diced bacon imported from Aliments Prince to be positive for Listeria. The initial product represented by that sample was refused entry. An in-depth investigation by the firm and the Canadian Food Inspection Agency into the root cause of the Listeria monocytogenes finding resulted in a recall of all precooked bacon products from the Canadian firm. The FSIS and the company have received no reports of illnesses associated with consumption of these products. Source: http://www.foodpoisonjournal.com/food-recall/two-recalls-announced-due-to-listeria-contamination/

National Beef recalls 60,424 lbs ground beef for e.coli. The U.S. Department of Agriculture (USDA) said National Beef Packing Co recalled about 60,424 pounds of ground beef products after inspection at an Ohio processing plant produced suspicions of contamination by e.coli 0157:H7 bacteria. The USDA and the company, based in Dodge City, Kansas, received no reports of illnesses associated with consumption of these products. The beef was shipped to distributors nationwide for further processing and distribution, the USDA stated. Winn-Dixie Stores, of Jacksonville, Florida, said it issued its own recall to customers tied to the recall, and said some of the beef affected was sold in its stores in Florida, Georgia, Alabama, Mississippi, and Louisiana. The beef had "sell by" dates of July 31 to August 12, it said. Colorado Sam's Club stores also contacted members who may have purchased beef included in the recall, a spokesperson for Sam's Club told the Colorado Springs Gazette. The problem was discovered as a result of routine microbial testing conducted by the Ohio Department of Agriculture at a state-inspected facility that had purchased these products for further processing, the USDA said. Source: http://www.baltimoresun.com/news/nation-world/sns-rt-us-food-beef-recalltre77e0hb-20110814,0,7955004.story

Government Sector (including Schools and Universities)

(Alaska) **Student arrested, accused of having gun on school bus.** An Anchorage, Alaska, high school student was arrested August 18 after he was found carrying a loaded gun on a school bus, authorities said. The 19-year-old had a .22 caliber handgun with him as he rode a bus from a local high school to a nearby vocational-education center, Anchorage School District officials said. “As the student was getting off of the bus, the driver noticed the student had a weapon,” said the district’s spokeswoman, adding that police were called and the student was turned over to their custody. The Anchorage student was in jail August 18 facing a charge of misconduct involving a weapon, an Anchorage Police Department spokeswoman said. The school district said in a statement it would be seeking to expel the student under a zero-tolerance policy concerning weapons. Source: http://af.reuters.com/article/oddlyEnoughNews/idAFTRE77I3AC20110819

(New Mexico) **Explosives found at school bus stop.** Police discovered an abandoned backpack filled with Molotov cocktails the morning of August 16 at a high school bus stop located less

than half a mile from Los Lunas Middle School in Los Lunas, New Mexico. A lieutenant said a sergeant was conducting routine patrols when he spotted the backpack at the corner of Los Lentes and Aspen around 4 a.m. “Inside were two bottles with rags coming out of the top and some sort of liquid,” he said. The Los Lunas fire inspector confirmed the devices inside were indeed Molotov cocktails. The entire backpack was sent to a crime lab in Las Cruces. Investigators are looking at security tapes from cameras on school buses to see if they can spot any students with the backpack. Police said they do not have leads to any possible suspects. Source: http://www.krqe.com/dpp/news/crime/explosives-found-at-school-bus-stop

(District of Columbia) **Police: Woman attacks art at DC museum again.** A woman who attacked a painting at Washington D.C.'s National Gallery of Art earlier this year has struck again, police said, this time lashing out against a Henri Matisse painting at the museum. The woman of Alexandria, Virgina, was arrested August 5 after police said she walked over to Matisse's 1919 painting "The Plumed Hat," and slammed the painting repeatedly against a wall, damaging its frame, but not the $2.5 million painting. The 53-year-old woman was arrested in April for attacking an $80 million Paul Gauguin painting called "Two Tahitian Women." As a condition of her release she promised she would stay away from all museums and art galleries in Washington. In the latest incident, reported August 15 by the Associated Press, she was charged with unlawful entry and brought to the city's mental health facility. Source: http://www.sacbee.com/2011/08/15/3838428/police-woman-attacks-art-at-dc.html

Information Technology and Telecommunications

Some mobile trojans are part of commercial spying services. Security researchers from Trend Micro identified a commercial service offered by a Chinese Web site that allows people to distribute a mobile trojan and receive the data stolen by it. The service's customers have the ability to customize the trojan and input the victim's phone number. This will lead to a malicious MMS being sent to the targeted individual. If the trojan is successfully deployed, the attacker can see the information sent back to the command and control service through the Web portal. The stolen data includes SMS messages, phone calls, GPS location, and e-mail messages. According to the Trend Micro researchers, the service costs $300 to $540. The trojan currently works on Symbian and Windows Mobile, but security experts are expecting an Android version to be launched too, especially since trojans with similar characteristics have been observed on Google's platform. Source: http://news.softpedia.com/news/Some-Android-Trojans-Are-Part-of-Commercial-Surveillance-Services-217726.shtml

New DroidDreamLight variant found in Android Market. Security researchers from Trend Micro identified a new variant of the DroidDreamLight trojan posing as an APK management app in Google's official Android Market. The trojanized app is called App Installer and had been downloaded 50 to 100 times before being removed by Google's staff. Upon installation, the app registers a service called AppUseService that is started every time a phone call is initiated or

received. The app sends device identification data such as model, IMEI, IMSI, language, and country to a command and control server. A list of installed apps together with their version is also uploaded. This variant uses another name for the encrypted configuration file, however, the DES encryption key is the same as in previous versions. Because the trojan does not use a root exploit to deploy its components, the Trend Micro researchers believe that it employs social engineering to trick users into installing it. Source: http://news.softpedia.com/news/New-DroidDreamLight-Variant-Found-in-Android-Market-217851.shtml

Koobface spreads via torrents. Security researchers identified a new version of the Koobface worm, which uses the global torrent network instead of social networking Web sites to spread. Dating back to July 2008, Koobface is one of the oldest and most successful computer worms that is still active. Its original variants targeted MySpace and Facebook, but it later expanded to other social networking sites. Koobface has seen many improvements and is a fairly sophisticated piece of malware most likely maintained by more than one developer. Despite its success, the worm suddenly stopped spreading on Facebook in February, a decision that baffled security researchers. In April, security experts from FireEye reported Koobface was still serving as a distribution platform for other malware, and that its command and control servers were still operational. A new sample found recently by security researchers from Trend Micro seems to indicate the worm's creators developed a new propagation routine. The new version bundles version 2.2.1 of the uTorrent client which runs hidden in the background to seed trojanized torrents. These torrents pose as cracked versions of popular applications or games. The new version also uses encryption to evade antivirus detection. The rogue torrents promoted via public trackers and discoverable through the global torrent network contain multiple components that decrypt each other. Source: http://news.softpedia.com/news/Koobface-Spreads-via-Torrents-217517.shtml

New mass injection attack infects over 20K Websites. Researchers from Armorize detected a new mass injection attack that affected over 22,000 Web sites so far, and directs users to drive-by download exploits. The researchers were able to determine the number of affected domains because the attackers originally forgot a script tag, rendering their code inactive. This meant search engine crawlers were able to index the code as regular text and make it searchable, allowing Armorize to find it on over 536,000 unique pages. The attackers have since fixed their injection. It is probable at least the 22,000 Web sites were reinfected with the proper code. When accessing a page compromised by this attack, visitors are redirected to a Web site hosting an installation of the BlackHole exploit pack. BlackHole executes exploits that target vulnerabilities in outdated versions of Java, Adobe Reader, Flash Player, and Windows itself. These attacked are called drive-by downloads and are generally transparent to victims. If they are successful, malware is download and installed on targeted computers. According to Armorize, the malware here is a fake antivirus application that uses the names "XP Security 2012" under Windows XP, "Vista Antivirus 2012" under Windows Vista, and "Win 7 Antivirus 2012" under Windows 7. The researchers believe attackers are using FTP credentials stolen from infected computers to compromise Web sites and inject code into their pages. Source:

http://news.softpedia.com/news/New-Mass-Injection-Attack-Infects-over-20K-Websites-217168.shtml

Google highlights trouble in detecting Web-based malware. Google issued a new study August 17 detailing how it is becoming more difficult to identify malicious Web sites and attacks, with antivirus software proving to be an ineffective defense against new ones. The company's engineers analyzed 4 years worth of data comprising 8 million Web sites and 160 million Web pages from its Safe Browsing service, which is an application programming interface (API) that feeds data into Google's Chrome browser and Firefox and warns users when they hit a Web site loaded with malware. Google said it displays 3 million warnings of unsafe Web sites to 400 million users a day. The company scans the Web, using several methods to figure out if a site is malicious. The detection process is becoming more difficult due to a variety of evasion techniques employed by attackers that are designed to stop their Web sites from being flagged as bad, according to the report. Source: http://www.computerworld.com/s/article/9219290/Google_highlights_trouble_in_detecting_web_based_malware

Report: More cyberattacks hitting social networks. Cybercriminals are increasingly targeting social networks, prompting users to take more steps to protect their online privacy, according to a Webroot study released August 16. In a survey of 4,000 social network users in the United States., England, and Australia, Webroot found the number of people hit by Koobface and other social networking malware rose to 18 percent this year from 13 percent last year, and 8 percent in 2009. In the United Kingdom specifically, the number of social networks hit by attacks climbed to 15 percent this year from 12 percent last year, and 6 percent the prior year. One notable attack that has grown more popular is the "friend in distress" scam in which a cybercrook claims to be a friend stuck in a foreign country in need of money. In the United States, this type of online con job was directed toward 14 percent of those polled this year, compared with just 2 percent in 2009, Webroot reported. Source: http://news.cnet.com/8301-1009_3-20093487-83/report-more-cyberattacks-hitting-social-networks/

Data thieves target hotels and resorts. Business travelers who books hotel rooms via the Internet may be at higher risk of being victimized by computer hackers and identity thieves, according to an article by the Los Angeles Times August 15. Insurance claims for data theft worldwide jumped 56 percent in 2010, with a bigger number of those attacks targeting the hospitality industry, according to a new report by Willis Group Holdings, a British insurance firm. The report said the largest share of cyber attacks — 38 percent — were aimed at hotels, resorts, and tour companies. That could spell trouble for business travelers who submit credit card numbers and other personal information to hotel Web sites, said a global markets leisure practice leader for Willis. She said large hotel chains are most vulnerable because hotel management companies may not be able to monitor how data is collected and stored at dozens or even hundreds of properties throughout the world. Independent contractors who work for individual hotels can also open the door to hackers and computer viruses, she said. Source: http://www.chicagotribune.com/travel/la-fi-travel-briefcase-20110815,0,984201.story

Man reveals secret recipe behind undeletable cookies. A privacy researcher has revealed the evil genius behind a for-profit Web analytics service capable of following users across more than 500 sites, even when all cookie storage was disabled and sites were viewed using a browser's privacy mode. The technique, which worked with sites including Hulu, Spotify, and GigaOm, is controversial because it allowed analytics startup KISSmetrics to construct detailed browsing histories even when users went through considerable trouble to prevent tracking of the Web sites they viewed. It had the ability to resurrect cookies that were deleted, and could also compile a user's browsing history across two or more different browsers. It came to light only after academic researchers published a paper late last month. The KISSmetrics CEO responded with a post on the firm's Web site claiming the research “significantly distorts our technology and business practices.” The company also added a ”consumer-level opt-out for those who wish to be entirely removed from all KISSmetrics tracking. One of the researchers stands by the findings and said KISSmetrics' recently updated privacy policy does not make it clear how users go about opting out of tracking. The researcher said the only way to block the tracking using the technique is to block all cookies and to clear the browser cache after each site visited. Source:
http://www.theregister.co.uk/2011/08/16/cookie_respawning_secrets_revealed/

Attack targeting open-source Web app keeps growing. An attack targeting sites running unpatched versions of the osCommerce web application keeps growing virally, more than 3 weeks after a security firm warned it was being used to install malware on the computers of unsuspecting users. When researchers from Armorize first spotted the exploit July 24, they estimated it had injected malicious links into about 91,000 Web pages. By early last week, The Register reported it had taken hold of almost 5 million pages. As of August 13, Google searches suggested that the number exceeded 8.3 million. Armorize said attackers were exploiting three separate vulnerabilities in the open source store-management application, including one discovered last month. The lead developer of osCommerce said there is only one vulnerability that is being exploited, but he said no one on his team had spoken to anyone at Armorize to reconcile the difference of opinion. He said a fix has been available since November's release of osCommerce Online Merchant v2.3. Source:
http://www.theregister.co.uk/2011/08/13/oscommerce_infection_threatens_web/

New Android spyware threat disguises itself as Google+ app. Security researchers from Trend Micro warn of a new information stealing Android trojan that disguises itself as an app for Google's new social product Google+. This latest threat is a variant of a recently discovered trojan called ANDROIDOS_NICKISPY which is able to record phone calls. This new version stands apart from the rest because it is capable of answering incoming calls if the phone's screen is turned off and if the calls originate from a number predefined by the attackers. "From the looks of it, the developer of this app went for the more real-time kind of eavesdropping as well, apart from the one ANDROIDOS_NICKISPY.A used, which involved recording calls," the Trend Micro researchers wrote. "The 'auto-answering' function of this malicious Android app works only on Android 2.2 and below since the MODIFY_PHONE_STATE permission was disabled in Android 2.3," they added. In addition to phone call answering and recording, the trojan has a full set of spyware features, such as stealing text messages and call logs or monitoring the GPS location.

The increasing sophistication and prevalence of Android malware reinforces the need of antivirus products for such devices. There are several free solutions from vendors such as AVG, Lookout, BitDefender, or Symantec. Source: http://news.softpedia.com/news/New-Android-Spyware-Threat-Disguises-Itself-as-Google-App-216757.shtml

Suspected Chinese spear-phishing attacks continue to hit Gmail users. Months after Google said Chinese hackers were targeting the Gmail accounts of senior U.S. government officials, attempts to hijack Gmail inboxes continue, a researcher said August 12. "Once compromises happen and are covered in the news, they do not disappear and attackers do not give up or stop. They continue their business as usual," said an independent security researcher based in Washington, D.C., on her Contagio Malware Dump Web site. In early June, Google announced it had disrupted a targeted phishing campaign designed to compromise Gmail accounts belonging to senior U.S. and South Korean government officials, military personnel, Chinese activists, and journalists. Google said it had traced the attacks to Jinan, China, a city in eastern China that has been linked to other hacking campaigns, including one in late 2009 against Google's own network. China denied accusations its government played a role in the attacks that accessed hundreds of accounts. And the attacks have not stopped. "Attackers ... continue their efforts with very slight modifications to the original themes," said the researcher. The latest campaign baits the scam with the promise of a report titled "Blinded: The Decline of U.S. Earth Monitoring Capabilities and its Consequences for National Security" from the Center for a New American Security (CNAS), a Washington D.C. think tank. In fact, CNAS offers that report as a free PDF download. The e-mails are customized for each recipient, and appear aimed at people associated with political and international affairs. Source: http://www.computerworld.com/s/article/9219155/Suspected_Chinese_spear_phishing_attacks_continue_to_hit_Gmail_users

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

Nothing Significant to Report

Public Health

Healthcare providers face 'record rates' of drug shortages. Research from healthcare consortium, Premier healthcare alliance, of unsolicited sales offers made by gray market vendors to hospitals, shows the average mark-up for shortage drugs was 650 percent. The highest single recorded mark-up offered was 4,533 percent for a drug used to treat high blood pressure. Normally priced at $25.90, the offered price in this case was $1,200. The analysis noted that some "gray market" vendors are putting profits ahead of patients, offering drugs desperately needed at exorbitant price mark-ups. And in certain cases, the drugs being offered

may be counterfeit, stolen, ineffective or unsafe, according to the report. Healthcare providers in the United state have to cope with “record rates” of drug shortages, market watchers have warned. Premier cited research from the University of Utah that forecasts more than 360 products reaching shortage levels by the end of the year, the highest in history. Analysis from the American Hospital Association, American Society of Health-System Pharmacists, University of Michigan and Premier found the vast majority of hospitals nationwide are experiencing life-threatening shortages of medicines needed to provide essential patient care. Combined, these analysis suggest the shortage could cost U.S. hospitals at least $416 million annually through the purchase of more expensive generic or therapeutic substitutes, and enhanced labor costs. Source: http://www.procurementleaders.com/news/latestnews/3308-healthcare-drug-shortages/

(Maryland) **Health department failed to control birth certificates, auditors find, citing possible fraud.** The Maryland Office of Legislative Audits issued a report August 18 saying it found the Maryland State Health Department has continued to fail to control issuance of birth certificates, leading to potential fraud. The Maryland Department of Health and Mental Hygiene has been unable to verify that birth and death certificates contain valid information, that certificates were only issued to the right people, and that payments for certificates were correctly collected. The state attorney general is investigating an employee in one local health department’s office for potential fraud. A legislative auditor said that serious problems with vital records have been found — and not corrected — in departmental audits since 1999. “These documents can be used for other things,” he said. “This is not just about the money involved. There is potential for immigration fraud.” Source: http://baltimore.citybizlist.com/1/2011/8/19/Health-Department-Failed-To-Control-Birth-Certificates-Auditors-Find-Citing-Possible-Fraud--By-Megan-Poinski.aspx

Drug shortages set to reach record levels. Hospitals are running out of drugs used in everything from cancer to surgery, anesthesia and intravenous feeding, the Food and Drug Administration (FDA) said. So far this year, 180 drugs have been in short supply, USA Today reported August 15. Virtually all U.S. hospitals say they have been affected, and 82 percent said the problem has delayed care for patients, says the American Hospital Association. Although drugmakers said they are doing everything they can to relieve the shortages, some health care experts say they see no end in sight. Drug shortages are also driving up prices, forcing hospitals to spend 10 times the usual amount, said the executive vice president at the Institute for Safe Medication Practices. The vice president of research at the Leukemia & Lymphoma Society said the shortages stem from changes in the ways drugs are made and regulated. Most hard-to-find medications are liquid, injectable drugs that must be kept sterile, according to the FDA. These drugs are more complicated to manufacture, store and ship than pills or tablets, an FDA spokeswoman said. In many cases, manufacturers have had to pull drugs because of "severe quality issues," such as particles or crystals in liquid medications. Most of the drugs in short supply are older, generic therapies, for which profits are much smaller than those of more expensive, brand-name drugs. About 80 percent of the raw materials for drugs are imported. That provides more opportunities for shipments to be delayed. Consolidation in the generic drug business has left fewer companies making each drug. In some cases, only one or two

companies may make an individual drug, said a spokesman for Illinois-based generic drugmaker Hospira. Drug companies are not required to notify the FDA or other regulators about shortages or delays, said the director of the Consumer Reports Health Ratings Center. Drugmakers must alert the FDA only if they plan to discontinue a "medically necessary" drug for which they are the only supplier. And while the FDA asks companies to voluntarily provide as much data as possible, drugmakers do not have to reveal the cause of the delay or when they expect to resume production.
Source: http://yourlife.usatoday.com/health/story/2011/08/Drug-shortages-set-to-reach-record-levels/49984446/1

TRANSPORTATION

TSA improves wireless cybersecurity after IG audit. The Transportation Security Administration (TSA) recently adopted improvements in practices to patch and configure software on its wireless networks to improve cybersecurity, following recommendations of the inspector general (IG) at the DHS. The IG conducted an audit of TSA wireless networks and devices such as Blackberries earlier this year to examine protections for sensitive information and other data on TSA networks. The audit revealed that TSA effectively protected its wireless network and devices generally with physical and logical security access controls, thereby avoiding any major vulnerabilities inherent with its wireless infrastructure. "However, we identified high-risk vulnerabilities involving patch and configuration controls," said the IG office in its report, Improvements in Patch and Configuration Management Controls Can Better Protect TSA's Wireless Network and Devices. The IG office made specific recommendations to TSA to revise its patch management process to patch software in a timely manner, and to enforce security policy for those individuals who do not properly secure their wireless systems and devices. In response to the report, the TSA Administrator said his agency already has enacted corrective measures. Source: http://www.hstoday.us/briefings/today-s-news-analysis/single-article/tsa-improves-wireless-cybersecurity-after-ig-audit/bfbb824d3c2fac205ac7abcfe8fd2988.html

(Washington) **Suspicious device found after train kills Seattle woman.** A busy passenger and freight rail line was shut down for nearly 5 hours August 18 after police investigating the death of a woman struck by a train in Seattle said they found a possible explosive near the tracks. Authorities later determined the woman had nothing to do with the device, which resembled a pipe bomb, a Burlington Northern Santa Fe (BNSF) railway spokesman said. He said experts now believe the object found near the woman's body to be a "firework-type device," although it was still being examined. The incident began at about 9 a.m. when the woman was struck near a Seattle park by a 63-car Burlington Northern freight train headed to Tacoma, Washington from Chicago, the spokesman said. Train operators who saw the woman sounded the locomotive's horn and went into an emergency braking operation but were unable to stop in time. Police found the device, prompting a shut down of the rail line used by 40 trains daily and which serves as a main connection to Canada. Three freight trains and one Amtrak passenger train were delayed before the line was reopened shortly before 2 p.m. The woman's death marked the fourth fatality on Seattle-area tracks since August 5. Source: http://news.yahoo.com/possible-bomb-found-near-seattle-train-tracks-193941798.html

(Wisconsin; Iowa) **Bridge over Mississippi River near De Soto closed due to cracks found in deck.** A bridge over the Mississippi River is closed near De Soto in southwest Wisconsin after transportation workers in neighboring Iowa found a crack in a floor beam under the bridge's deck. The crack was discovered August 17 during a routine inspection of the bridge on Iowa's Highway Nine between Lansing and De Soto. Iowa's department of transportation does not know how long the structure will be closed. The nearest open bridges on the Mississippi are 30 miles away in either direction at La Crosse and Prairie du Chien. Source: http://www.piercecountyherald.com/event/article/id/38396/group/News/

(Arizona) **Three Africans charged over fake bomb at Phoenix airport.** Three Africans were charged August 12 with trying to sneak a fake bomb past a screening area at a Phoenix airport, in what the FBI describes as a possible test of security. A criminal complaint filed in federal court in Arizona also states the discovery of the suspicious item, which was a candy box with a cell phone attached, was made within days of a similar incident at a Memphis, Tennessee airport. The suspect was arrested at Sky Harbor Airport in Phoenix August 5 after Transportation Security Administration (TSA) officers X-rayed her carry-on bag and noticed an object that at first sight appeared to be an explosive, an FBI special agent said in the complaint. After investigators spoke to the suspect, they traced the object to two individuals who both live in Phoenix, and arrested them. The complaint does not detail any other possible connection between the incidents in Phoenix and Memphis, and it does not accuse the three Africans of being part of a terrorist organization. Prosecutors were going to seek further detention for all three individuals, the U.S. attorney's office said. Source: http://www.reuters.com/article/2011/08/13/us-plane-threat-idUSTRE77C0AL20110813

(Ohio) **Conneaut: Bomb found on railroad tracks at Mill Street.** The Conneaut, Ohio assistant fire chief said a small bomb the "size of a cigarette pack" was discovered about 10 a.m. August 14 on the Norfolk Southern railroad tracks at Mill Street. Conneaut police and fire departments shut down Mill Street and stopped all train traffic traveling the tracks between Cleveland, Ohio and Buffalo, New York for several hours. The Lake County Sheriff's Department sent its bomb squad to the scene at the request of the Conneaut police department. The Geauga County sheriff's department was also asked to send one of their K-9 units. The bomb squad used a robotic device to retrieve the bomb and detonate it. The bomb was wrapped in duct tape with a fuse attached, but the fuse had gone out. The bomb contained gunpowder, pennies, and BBs. The assistant fire chief said that, had it detonated, it would not have likely caused any damage to a train, but the shrapnel would have caused damage to a passing car or injured a person walking by when it exploded. Source: http://www.wkyc.com/news/article/202099/45/Conneaut-Bomb-found-on-railroad-tracks-at-Mill-Street

(California) **Hackers protest BART decision to block cellphones.** San Francisco's mass transit system prepared for renewed protests August 15, a day after hackers angry over blocked cell phone service at some transit stations broke into a Web site and posted company contact information for more than 2,000 customers. The action by a hacker group known as

Anonymous was the latest showdown between anarchists angry at perceived attempts to limit free speech, and officials trying to control protests that grow out of social networking and have the potential to become violent. Anonymous posted people's names, phone numbers, and street and e-mail addresses on its own Web site, while also calling for a disruption of the Bay Area Rapid Transit's (BART) evening commute August 15. BART officials said August 14 they were working a strategy to try to block any efforts by protesters to try to disrupt the service. The transit agency disabled the effected Web site August 14 after it also had been altered by apparent hackers who posted images of the so-called Guy Fawkes masks that anarchists have previously worn when showing up to physical protests. The cyber attack came in response to the BART's decision to block wireless service in several of its San Francisco stations August 11 as the agency aimed to thwart a planned protest over a transit police shooting. Officials said the protest had been designed to disrupt the evening commute. Source: http://www.boston.com/business/technology/articles/2011/08/15/hackers_protest_bart_decision_to_block_cellphones/

Water and Dams

(Nebraska) **E.coli detected in Wahoo water.** The City of Wahoo, Nebraska, issued a boil water notice August 17 after an E.coli organism was detected during a test. The notice is effective for the entire water system, which includes Wahoo and Colon. The general manager of the Wahoo Utilities Department said the organism was found in one spot in the downtown business district. “We have immediately started to chlorinate our water, and we will have to chlorinate it for 10 days,” the manager said. Normally, the city does not add treatment to its water. The source of the E. coli bacteria is thought to be water mains because many breaks have occurred during the last 2 or 3 weeks. When mains are repaired, they are normally disinfected and flushed, but officials suspect when the mains were repaired they did not get cleaned entirely. Source: http://fremonttribune.com/news/local/article_6408dbaa-c920-11e0-8c42-001cc4c03286.html

(Virginia) **CDC seeks to sample Virginia waters for deadly amoeba.** The U.S. Centers for Disease Control and Prevention (CDC) is attempting to develop a test for detecting microscopic amoebas that caused three U.S. deaths this year. One victim visited several bodies of water during a Richmond, Virginia fishing camp the previous week, while a Louisiana man and a Florida girl also died after exposure to the amoeba this summer. In total, more than 120 people have died of the waterborne amoeba since it was identified in the early 1960s, the CDC reports. The CDC knows little about the free-living amoebas, which can be found in bodies of freshwater around the country, said the federal agency's associate director for healthy water. The Atlanta-based agency would like to know why millions of people come in contact with the amoebas every year by swimming in their local ponds and lakes, but only a few die. Officials said the test being developed would use an antibody that would act as a magnet to pull the amoeba out of a volume of water. Source: http://www2.timesdispatch.com/news/news/2011/aug/20/tdmet01-cdc-seeks-to-sample-virginia-waters-for-de-ar-1250285/

Brain-eating amoebas blamed in three deaths. Three people have died this summer after suffering rare infections from a waterborne amoeba that destroys the brain. The amoebas, called Naegleria fowleri, flourish in the heat — especially during the summer months in the south, thriving in warm waters where people swim. It is the only type that infects humans, and it is more than 95 percent lethal. The first death in 2011 occurred in June in Louisiana, according to the U.S. Centers for Disease Control and Prevention. A 16-year-old died August 13 after becoming infected by an amoeba in Brevard County, Florida, according to a CNN affiliate. The teenager suffered a fever, nausea, and headaches, and a spinal tap showed Naegleria fowleri was present in her spinal fluids. In another case, the Virginia Department of Health confirmed August 12 a 9-year-old boy from Henrico County, Virginia, died from primary amoebic meningoencephalitis, which is caused by the amoeba. The amoebas enter the human body through the nose after an individual swims or dives into warm fresh water, such as ponds, lakes, rivers, and even hot springs. A human is an "accidental end point for the amoeba after it is forced up the nose," a scientist said. It does not seek human hosts and it is not a parasite. But when an amoeba gets lodged into a person's nose, it starts looking for food. It ends up in the brain and starts eating neurons. Early symptoms include headache, fever, nausea, vomiting and neck stiffness. Later symptoms include confusion, lack of attention to people and surroundings, loss of balance, seizures, and hallucinations. The amoeba multiplies, and the body mounts a defense against the infection. This, combined with the rapidly increasing amoebas, causes the brain to swell, creating immense pressure and the brain stops working. Death typically occurs 3 to 7 days after symptoms start. Source: http://www.cnn.com/2011/HEALTH/08/17/amoeba.kids.deaths/index.html?hpt=hp_t2

(Utah) **Suspicious activity prompts investigation at Echo Dam.** Witnesses at the Echo Resort in Coalville, Utah, said a group of men arrived at the Echo Dam early August 7, KSL-TV 5 Salt Lake City reported August 16. They paid a resort worker $35 to launch at least two boats. Several of the men remained on shore while others piloted their boats to the dam and spent hours shining lights along the width of the structure. They were gone by daylight. The resort employee mentioned it to his boss later the next day, and the boss called police. "Well it certainly was an unusual event," said a spokesman for the U.S. Bureau of Reclamation, which oversees Echo Dam and numerous other dams in Utah. The witnesses said the men did not appear to be from the United States. Summit County sheriff's deputies, along with federal authorities, were on the scene the next morning. The dam was deemed safe. Witnesses at the resort said authorities used what appeared to be a remote submarine to check out the dam under the surface. Echo Resort enhanced security and printed up flyers for campers describing the event and asking them to be on the lookout. Source: http://www.ksl.com/?nid=148&sid=16825521

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168